Service Level Agreement (SLA)

for the

Access to Archival Databases (AAD) Project

February 7, 2006

National Archives and
Records Administration (NARA)
8601 Adelphi Road
College Park, MD 20740-6001

This page intentionally left blank

Table of Contents

This page intentionally left blank

Service Level Agreement (SLA)
for the
Access to Archival Databases (AAD) Project

1. Executive Summary

The purpose of this Service Level Agreement (SLA) is to detail the conditions of the service contract between the National Archives and Records Administration (NARA) and the vendor to provide hosting and application support services at the vendor's facilities for the AAD test bed, staff-only, and public subsystems. The duration of this SLA is the period from the date that NARA awards the contract and the vendor has taken charge of the AAD systems, or when superseded in the next version of this SLA. The ownership of the agreed upon service levels belong to Kenneth Grant, the NARA AAD Project Manager; and the NARA Director of the Center for Electronic Records (NWME), the owner of the AAD system.

2. Scope and Intent of this Agreement

This Service Level Agreement (SLA) details the conditions of the service contract between the National Archives and Records Administration (NARA) and the vendor to provide hosting and application support services at the vendor's facilities for the AAD test bed, staff-only, and public subsystems.

The test bed consists of the developmental versions of the following modules: the Metadata Completion Tool, the Records Description Tool, the Browse Search and Retrieval Module, and the public staging server and FTP server. The staff-only subsystem consists of the Metadata Completion Tool (MCT), the Records Description Tool (RDT), and the Browse, Search, and Retrieval (BSR) module with staff-only and public staging server components. The AAD public system consists of the Browse, Search, and Retrieval (BSR) module running in a high-performance and high network bandwidth environment.

This document describes the services and standards of service to be provided by the vendor and is intended to guarantee that NARA receives an acceptable level of performance and availability of services within the AAD environment. Hence, this document is an agreement defining acceptable levels of service and support from the vendor to NARA for the AAD environment.

The vendor shall make a good faith effort to meet or exceed the service levels identified below. The service levels and their measurements are intended to measure whether or not the vendor is meeting acceptable performance levels.

The scope of this service-level agreement is to provide the following services to NARA at the specified service levels:

- **Data Center Services –** To undertake overall systems and network management, backup/recovery activities and ongoing system administration for the AAD systems.
- **Software Development Services –** To provide ongoing system enhancements, patches and bug fixes for the AAD system.
- **Production Control Services –** To ensure scheduled tasks such as data loading, indexing, metadata completion, replication to the public server, and general support services are completed on schedule and reports are delivered on time.

.

3. Term of Agreement

This agreement is valid for the period from the date that NARA awards the contract and instructs the vendor to take over AAD. The start date is consistent with the current award of the AAD contract and the stop date coincides with the end of the first option year in the contract.

4. Review and Reporting Process

The vendor is committed to delivering quality IT services to NARA. This document is intended to represent the AAD system service level requirements. As such, the vendor services provided should be the subject of monthly performance reviews between NARA and the vendor. Performance reviews will be conducted weekly for the first month of the SLA. The weekly reviews may be extended beyond the first month of the SLA at the discretion of the NARA PM. The details of the agreement will be reviewed at regular intervals and may be amended as required, provided such amendments have been agreed to by the vendor and NARA. During each review, actual service levels and costs will be compared with the commitments outlined in the service-level agreement.

4.1 Service-Level Performance Reporting Process

Service-level targets and their achievement will be documented via four (4) mechanisms including:

- Periodic and *ad hoc* reports on system performance and metrics as detailed herein
- The issuance and management of trouble reports
- The generation and delivery of exception reports on an as required basis for all incidents when service-level targets are not met.
- Monthly reviews of the SLA

Overview of Periodic and *ad hoc* Reporting Mechanism. NARA would like to know "how well the AAD system is doing" and public reaction to the system. Additionally, NARA is interested that proper security measures are in place to protect agency records and to provide for quality of service (QoS) to the public. Copies of the templates of the following reports appear in the appendices.

Accordingly, the vendor will provide the following periodic reports:

- Weekly Basis

    - Docket of metadata completion activity as discussed in the SOM
    - A statement affirming continuing system security and data integrity (including software integrity) and any integrity checks performed during the week
    - A statement affirming that required backups have been made during the week
    - Statistics on public use (from the “true” Public Site):
        - Number of “virtual visitors” (number of sessions) to the AAD Web site on a day-by-day basis during the week
        - Number of queries executed on a series-by-series basis for each day during the week
        - Web server and database server performance statistics averaged daily during the week
        - How many queries were successful and unsuccessful (i.e., those that resulted in an error message)
        - Number of times scanned technical information package items are downloaded
        - Number of times search results are downloaded as .csv files

- Monthly Basis

    - Rollup report regarding system security and data integrity
    - Rollup report regarding system backups
    - Rollup report of the weekly public use statistics
    - Synopsis of trouble reports made during the month
    - Synopsis of SLA exception reports made during the month
    - Monthly audit log summaries
    - Firewall and Intrusion Detection System (IDS) reports
    - Alerts and patches implemented
    - Configuration Status Accounting (CSA) Report

To the extent that information and data is captured as part of the server and firewall logs in the AAD system, the vendor will conduct *ad hoc* queries and provide reports as requested by the NARA AAD Project Manager.

Overview of Trouble Reporting Mechanism. Trouble reports will be generated on an as required basis. Either NARA or the vendor may submit a trouble report. Trouble reports shall not be used to request changes or enhancements to the system or network. By definition, trouble reports shall only be used whenever the system or network is experiencing problems of a nature that means that the system cannot be effectively used or a security violation has been noticed. Trouble reports can also be used for reporting problems with the metadata and/or agency data that has already been loaded and initially run through the metadata completion test script.

For NARA-generated trouble reports, trouble reports should be forwarded to the onsite vendor team leader with a copy to the vendor PM and the NARA PM. Initially, trouble reports will be submitted manually via e-mail. A configuration management tool will ultimately be implemented by the vendor providing NARA with an improved, on-line, Web-based mechanism for trouble reporting, trouble resolution, and change requests. This on-line mechanism will be done in accordance with the AAD Configuration Management Plan.

Trouble report types of issues that surface through interaction with the public (by e-mail or telephone) will be routed by NWME to the onsite vendor team leader, who will investigate the problem and generate a trouble report, as necessary. The vendor will report its findings to NWME, which will report the outcome to the public.

Subject to further development with NARA, the trouble report should contain the following information, as appropriate: (Note: See Appendix A for an MS Word template for a trouble report)

- Person making the trouble report should provide:

  - Subject of the trouble report
  - Who is reporting?
  - Type of report (e.g., Initial, Follow-on information, Closure) with information including the sequence (e.g., This is the 2nd report in the sequence)
  - Date and time first noted?
  - Where was the problem noted in the system (e.g., which page and on which subsystem or module)?
  - Nature of the problem?
  - Any special circumstances or conditions?
  - Screenshots (if appropriate)
  - Notes
  - Priority for resolution and escalation level (See Section 7.1)

- The vendor will respond with the following:

  - Any service-level metrics potentially impacted and if so, which?
  - Personnel assigned
  - Prognosis for the resolution of the trouble report (including expected date/time for resolution)
  - Trouble report closeout information – e.g., what was accomplished?

Service-Level Reporting Mechanism. This SLA acknowledges the possibility that individual trouble reports (or perhaps a collection of related trouble reports) may result in an assessment that mutually agreed-upon service levels are not being met. For example, the system could experience multiple short outages or problems during a given month, which when aggregated may mean that the overall system availability or performance was below established service level for the month.

The vendor will generate and deliver *ad hoc* SLA exception reports on an as required basis for all incidents when service-level targets are not being met, and when it first becomes apparent to the vendor that a service-level metric is not being achieved (e.g., “yellow” or “red” designation, as per sections 6.1-6.3.). Initially, the vehicle for notification and delivery of the exception reports will be via e-mail to the NARA Project Manager with follow-up action and resolution as necessary. As a configuration management tool is implemented it is anticipated that service level reporting will be further automated for the project.

Subject to further development with NARA, the *ad hoc* SLA exception report should contain the following information, as appropriate: (Note: See Appendix B for an MS Word template for an SLA Exception Report)

- Title or subject of the exception report
- Date and time the exception was noted
- Service impacted by the exception
- Assessment of the level of the exception (“Yellow” or “Red”)
- Nature of the service level exception
- Circumstances of the exception (e.g., including any mitigating circumstances?)
- Personnel assigned and actions implemented by the vendor
- Requested actions of NARA (if any)
- Prognosis for resolution of the exception (included projected date for resolution and return to “Green” status)

The vendor agrees to provide a synopsis of the SLA exception reports on a monthly basis, at the end of the month that will indicate performance against all targets for the month. During the first month of the SLA, however, the vendor will provide these reports on a weekly basis. This weekly reporting requirement may be extended at the discretion of the NARA PM.

4.2 Service-Level Review Process

The NARA AAD Project Manager will review the service-level targets and the status of their achievement on a monthly basis with the vendor. During the first month of the SLA, however, this review will occur on a weekly basis. This review process requirement may be extended at the discretion of the NARA PM. Elements of the monthly technical review process shall include:

- Review of the weekly/monthly synopsis of exception reports
- Review of specific exception reports as required
- Review of metadata completion activity as documented in the docket
- Review of public access metrics and associated performance statistics
- Review of trouble reports and their status
- Identify emerging requirements and plan technical changes
- Monitor resource use and costs against the service-level agreement
- Plan for system capacity and performance improvements
- Recommend modifications of the Service Level Agreement

5. O&M Environment for Providing ASP Services for AAD

To effectively support the NARA AAD Project objectives, it is imperative that consistent support and acceptable service levels be provided by the vendor. The support and services are primarily those required to provide comprehensive, end-to-end operations and maintenance (O&M) of the AAD system environment.

The vendor shall function as the AAD Application Service Provider (ASP) for both the public and NARA staff-only subsystems. The vendor shall provide ASP services primarily from its facility.

This facility must be a secure facility with adequate protection for certain sensitive project documentation and data which must be protected in accordance with the terms of the contract. The vendor must agree with these terms and conditions.

The following are the major operations and maintenance (O&M) design factors that are incorporated into this Service Level Agreement (SLA):

- The vendor is responsible for providing access and support to the AAD system in accordance with the service parameters defined in sections 6.1 - 6.3 of this SLA.

- The AAD Project is a tenant of the vendor's facilities with assigned spaces that are secured via normal door locks. The vendor will secure sensitive material assigned to the project at the same level that it does for its own business sensitive information.

- The vendor will supply the AAD Project with an internet connection for the AAD system.

- AAD connectivity to the public will be provided via an ISP (Internet Service Provider) at the vendor's site. Once again, the AAD Project is not responsible for the ISP connection or its overall operations and maintenance. Both the vendor and NARA accept the ISP's SLA as a part of the overall system design.

- The vendor further accepts that the ISP high-speed Internet connection shall be used solely for NARA AAD business. The following O&M factors apply to the overall system operation relative to the ISP:

    - The vendor certifies that the ISP connection shall be solely used for NARA AAD business. This statement is legally binding on the vendor, and the vendor's AAD Project Manager shall be responsible for ensuring compliance. Any other use of the ISP connection constitutes a misappropriation of government resources. Should it become apparent at any point that this policy is being violated, the vendor shall be bound to report the violation to NARA. In consultation with the NARA AAD Project Manager, the vendor shall institute sanctions and take appropriate administrative and personnel actions in accordance with the vendor's policy.

    - Specifics in physical connection to the ISP will be agreed upon and documented based upon the accepted proposal.

    - Lastly, the vendor accepts that NARA may conduct inspections, reviews, and audits of the dedicated ISP Internet connection as required.

- Both NARA and the vendor accept any limitations in AAD services associated with the following:

    - The current Internet connection speed for the NARA staff-only subsystem is equivalent to a T-1 line. The vendor will provide the Internet connection for the AAD project *gratis* (i.e., at no direct cost to the project). It is anticipated that a dedicated line for staff-only access may be required at additional cost to the project. Alternately, it may be possible (bandwidth and public demand permitting) to multiplex NARA staff-only access on the ISP connection.

    - Public utilities including electrical power and phone service to the building are outside of the control of the AAD Project. The AAD Project currently has uninterruptible power supplies (UPS) on all vital system components and network connections. The vendor AAD Project personnel shall have cellular phones that can be used as an alternative to terrestrial-based phone service in the building. Both NARA and the vendor recognize that if electrical power is lost for beyond but a few minutes, that the AAD services and the ISP connection may be interrupted. Under such circumstances, the AAD Project shall notify NARA via a trouble report that power has been lost and that the system is down. In the future, it may be necessary (at additional cost to the project) to provision additional electrical power backup capability potentially including a generator.

- The vendor will not be held responsible for loss of AAD services due to acts of nature and accidents other than to provide for backup and recovery services.

- The vendor will not be held responsible for loss of AAD services due to deliberate acts of man, including but not limited to sabotage and acts of terrorism. A *force majeure* clause shall be in effect.

5.1 Data Center Services

5.1.1 Configuration Management

The vendor will maintain the configuration of the AAD technical environment. The configuration will include a complete inventory of the AAD environment (e.g., hardware, software, and network resources) as well as the administrative procedures required for maintenance and support of the system. The AAD Systems Operation Manual (SOM) provides details on these procedures. Note: Additional aspects of configuration management will be under active development as a configuration management tool is implemented and coordinated with NARA.

5.1.2 Systems Monitoring and Maintenance

Consistent with the level of effort (LOE) in the contract, the vendor will provide overall systems monitoring and maintenance services. System monitoring and maintenance services will be provided during normal NARA business hours, which are defined as being from 8:00am-5:00pm, Eastern Time, Monday through Friday, federal holidays excepted.

5.1.2.1 Monitoring and Inspection of Logs

The vendor will inspect the AAD system at the beginning of each business day to ensure all appropriate processes are running, that there are no errors in the system error logs that adversely affect the mission of the system, that system integrity is preserved, and that sufficient disk/file system space is available. The vendor will also analyze trends from these logs over time and make appropriate recommendations to NARA as part of its weekly/monthly service level review process. If problems are detected during the daily checking, the vendor will take appropriate action to correct the problem and report the problem to the NARA AAD Project Manager.

On a daily basis (excluding weekends and federal holidays), the vendor will monitor and inspect the following logs for both the public and NARA staff-only systems:

- Firewall log for any evidence of intrusion activity
- Query log

- AAD Event log
- Oracle Audit Tool log
- FTP log

5.1.2.2 Hardware Monitoring and Management

The vendor will monitor the hardware in the AAD environment during normal business hours. If the vendor determines that a problem exists with the hardware, the vendor will coordinate repairs/replacements through the applicable contracts with the hardware vendors . Additionally, the vendor will report any hardware problems to the NARA AAD Project Manager.

5.1.2.3 Performance Monitoring and Tuning

The vendor will monitor system performance on all platforms within the AAD environment (during normal business hours) to ensure that they are operating within acceptable levels (see Section 6.1). If the monitoring process indicates a potential performance problem, the vendor will research the problem and make the appropriate adjustments to tune the system's performance, coordinating with the NARA AAD Project Manager as necessary.

Any changes requiring a production shutdown, including taking any particular series or file units offline, will be coordinated with the NARA AAD Project Manager in advance of taking these actions. In the event that portions of AAD are taken offline, the vendor will display to users an appropriate notice.

Consistent with the Requirements Document, both NARA and the vendor recognize that the end-to-end performance and quality-of-service (QoS) of the AAD system will naturally depend on a number of system-defined and user-defined factors that are highly dynamic in nature. Both NARA and the vendor acknowledge that a number of the factors may be outside the span of control of either or both the vendor and NARA. Accordingly, quality of service and performance, as perceived by the user community, shall be viewed as more of an “objective to be managed” than as a hard-and-fast timing requirement.

Both NARA and the vendor also recognize that certain adjustments may require hardware/software/network upgrades. These proposals will be vetted through the NARA Configuration Management process. The cost of the upgrades will be discussed and negotiated with NARA on a case-by-case basis.

5.1.3 Network Management Services

Consistent with the level of effort (LOE) in the contract and the ISP Service Level Agreement, the vendor will coordinate and manage network services for AAD. Network management services will be provided during normal NARA business hours.

Under this SLA, the vendor will provide network management services to include the following:

- Coordination with ISP provider for availability and performance management purposes up to the AAD server room for the public system. This effort will include surveillance and monitoring of the ISP.
- Coordination with the vendor provided network for availability and performance management purposes up to the vendor provided network demarcation point in the AAD server room for the NARA staff-only subsystem.
- Provision of a shared network connection (including providing firewall rule set management) via the vendor provided network for the NARA staff-only subsystem past the vendor provided network demarcation point.
- Management of the firewall and load balancing switch for the public subsystem.
- Operations and management of HTTP, FTP, and Windows Terminal Services as necessary for both the public and NARA staff-only subsystems.
- Overall network operations and configuration management for the AAD system past any vendor-provided and/or ISP-provided network demarcation points.
- Network fault isolation and resolution for the AAD system past any vendor-provided and/or ISP-provided demarcation points.
- Network performance troubleshooting and development of engineering recommendations for the entire AAD system to include resource and capacity planning.

5.1.4 Database Management Services

Consistent with the level of effort (LOE) in the contract, the vendor will provide overall database management services. Database management services will be provided during normal NARA business hours.

The vendor will provide a full range of database support services in accordance with the relevant current technical literature, such as Oracle 10g and Lucene technical and reference manuals and recommended practices on Oracle’s Metalink Web site:

- Install and upgrade Oracle database and application server software
- Provide data administration and data modeling support
- Perform physical database design and create database objects
- Maintain developmental database schemas
- Create production database schemas
- Migrate development and/or test data to production
- Develop initial load programs and utilities
- Develop database triggers and stored procedures
- Load and materialize agency databases
- Promote agency data from the public staging server to the public production system

- Index columns and run statistics
- Perform periodic database backups
- Establish and test database recovery routines
- On request, perform database unloads (e.g., deleting tables)
- Maintain overall database security
- Maintain database integrity via the Oracle Audit Tool
- Monitor the performance of the database environment
- Optimize the database (as necessary) via striping, defragmentation, re-indexing, etc.
- Maintain Lucene's full-featured text search engine library

5.1.5 Server Management Services

Consistent with the level of effort (LOE) in the contract, the vendor will provide overall server management services. Server management software will include embeded capabilities in the Sun Solaris operating system, Oracle (e.g., Oracle 10g Application Server and RDBMS), and Microsoft products (e.g., Microsoft Internet Information Server (IIS), Windows 2000 Server, and Windows Terminal Server). Server management services will be provided during normal NARA business hours.

The vendor will provide a full range of server management services as "best" commercial practices for the AAD system as listed below:

- Setup and configuration management and control of Oracle 10g Application Server (on the public subsystem) and Microsoft Internet Information Server (IIS) on the NARA staff-only subsystem.
- Setup and configuration management and control of Sun Solaris and Windows 2000 Server operating systems on appropriate platforms within the public and NARA staff-only subsystems.
- Daily monitoring of server event logs and query logs for security and performance monitoring/tuning purposes.
- Weekly monitoring and inspection of application code on the applications servers.
- Balancing load on the F5 Big-IP switch directed to the Sun Netras on the public subsystem as required.
- Developing and coordinating (with NARA) any scripts and associated Web pages necessary to divert potentially large numbers of public users to "other" parts of the system (e.g., pages that might say "come back later").

5.1.6 Security

5.1.6.1 Physical Security

The vendor shall provide the following physical security services:

- The vendor will ensure that all components that comprise the AAD environment are configured and maintained by authorized vendor personnel.

- The vendor will control physical access to the AAD server room that contains routers, firewalls, web-servers, database servers, and application servers. All spaces occupied by the AAD Project including office spaces in the building shall be under lock and key during non-business hours.

- The vendor will report any physical security compromises of the AAD system to the NARA AAD Project Manager within two (2) hours of their discovery.

5.1.6.2 Network Security

In addition to the physical security measures identified above, the vendor will provide additional network security via firewalls on the public subsystem and on the NARA staff-only subsystem as detailed below:

- **Staff-Only Subsystem.** On the staff-only subsystem, network security is currently provided via a Cisco Router and firewall that is part of the vendor provided network services and network connection to the Internet that the AAD Project accesses. In that regard, the AAD Project's connections to the Internet will operate on the vendors network and provide for a managed Internet connection to the vendors workgroups and their customers that is the functional equivalent of buying a separate Internet connection via an independent Internet Service Provider (ISP).

  As a managed service, security policy for access to the network will be under the control of the vendor's corporate IT staff. To use the connection, the AAD Project must function and operate within the bounds of a corporate security policy which requires that separate network security services (e.g., a firewall) be provided by the vendor's business units that use the connection. By the vendor's corporate policy, the following criteria must be met to operate and use the internet connection:

  - All systems must be adequately hardened for security.
  - Systems using the internet connection must be located on Local Area Networks (LANs) that are physically separate from the vendor provided network.

  As part of the vendor's corporate security policy, network devices are only allowed to use the connection under the following circumstances:

  - All network devices must be listed and approved by the vendor's Network Security.

- All systems must be adequately hardened for security. The Requestor has the responsibility for all measures required to ensure on an ongoing basis the security of the network devices.
- There must be a clear and reasonable business case for operating or using a network device. Each network device operated or used on the connection must have an existing business case based on a contractual obligation that is allowable within the vendor's security policies.
- Any network device that acts as a firewall must be approved by the vendor's Network Security. In certain cases approved firewalls may be different than the list of approved firewalls that are allowed to connect to the vendor provided network.
- Network devices must be configured to allow the vendor's Network Security to scan all devices and systems behind it.
- Network LANs behind network devices must be physically separate from the vendor provided network.
- The vendor's Network Security and/or the vendor's Network Operation Center (NOC) must have sufficient access to the device to verify the configuration, and shut down the device if necessary.
- If a network device on the connection or any system behind it becomes compromised and/or "hacked", the standard IP address blocking procedure will be enforced to prevent further attacks and to deny access to the attacker. This block will remain in place until the vendor's Network Security is able to verify that the affected system has been sanitized. Systems behind a blocked network device may or may not be affected, depending on the configuration of the system.
- If any of the systems behind the network device cannot be configured to a fixed public IP address, then Firewall Exceptions may not be allowed to or from that system.
- Network devices on the internet connection must be renewed every six months.

AAD Project Compliance. As a part of the AAD Project, the vendor also provides an additional software-based firewall under the direct control of the vendor's workgroup assigned to this project. This separate firewall monitors and filters incoming requests that pass the internet connection for HTTP, TELNET, FTP, SMTP traffic, etc. Before allowing access, the software-based firewall will check to see if the requested network service is authorized to connect to the AAD system. This separate software-based firewall must meet the vendor provided security requirements.

For the staff-only subsystem, the vendor will monitor the software-based firewall logs on a daily basis to determine if there are any intrusion attempts. Any intrusions (with a preliminary analysis of their impact) will be reported to the NARA AAD Project Manager within 2 hours of their discovery. If repeated unauthorized attempts to access the system are discovered (including denial of service attacks), the vendor will research the violation and will attempt to contact the host master of the sending IP address informing them that the activity must stopped immediately. As necessary, the vendor will report violations and suspicious activity to the appropriate civil authority.

- **Public Subsystem.** On the public system, network security past the ISP demarcation point will be provided via the F5 Big-IP load-balancing switch and firewall. This switch will be under the direct control of the vendor's workgroup assigned to this project. The switch will be configured in accordance with the SOM.

  For the public subsystem, the vendor will monitor the F5 Big-IP firewall log on a daily basis to determine if there are any intrusion attempts. As with the staff-only subsystem, any intrusions (with a preliminary analysis of their impact) will be reported to the NARA AAD Project Manager within 2 hours of their discovery during normal business hours. If repeated unauthorized attempts to access the system are discovered (including denial of service attacks), the vendor will research the violation and will attempt to contact the host master of the sending IP address informing them that the activity must stopped immediately. As necessary, the vendor will report violations and suspicious activity to the appropriate civil authority.

5.1.6.3 System Security Reporting

Under this SLA, the vendor shall provide the following system security reporting:

- To the extent that information and data is captured as part of the logs in the AAD system, the vendor will conduct *ad hoc* queries and provide reports of a security and data integrity nature as requested by the NARA AAD Project Manager.

- On a daily basis, the System Administrator will use auditing tools to look for any unauthorized changes to monitored data tables associated with agency electronic records. If unauthorized changes are detected, the System Administrator or the vendor Project Manager will notify the NARA Project Manager with recommendations for further action within two (2) hours of their discovery during normal business hours.

- On a weekly basis, the System Administrator will use auditing tools to detect any unauthorized changes on both the public and NARA Staff-only databases. These weekly audits will be applied to functions, stored procedures, triggers, and sequences. Specifically, functions, stored procedures, triggers, and sequences will be monitored and checked for the following unauthorized database actions:

  - Insert
  - Update
  - Delete

If unauthorized changes are detected in the functions, stored procedures, triggers, and sequences within the system, the System Administrator or the vendor Project Manager will notify the NARA Project Manager with recommendations for further action within two (2) hours of their discovery during normal business hours.

- On a weekly basis, the vendor Project Manager and the System Administrator will verify the integrity of the AAD applications code in both the public and NARA staff-only subsystems using a digital signature mechanism as discussed in the SOM. If unauthorized changes are detected in the applications code, the vendor Project Manager will notify the NARA Project Manager with recommendations for further action within two (2) hours of the discovery during normal business hours.

- On a weekly basis, the vendor Project Manager will send an e-mail to the NARA AAD Project Manager verifying and affirming that required security and integrity checks have been made for the week and summarizing any adverse findings.

5.1.7 Backup and Recovery Operations

The vendor is responsible for backup and recovery operations as discussed in this section. On a weekly basis, the vendor Project Manager shall provide a report to the NARA AAD Project Manager verifying that backup operations have been performed as specified in this section of the SLA.

As part of the SLA, the following requirements are established for backup and recovery as well as future disaster recovery planning:

5.1.7.1 Daily Backup and Recovery

Effective immediately, the vendor shall perform a daily (e.g., Monday – Friday) backup of the complete AAD Configuration and Object Database (e.g., AAD schema) for the NARA staff-only subsystem, the public subsystem, and the testbed. Provisions include:

- Backup all objects as defined in Table 1

- Store the backup of Table 1 objects onsite at the vendors site in the following logical formats:

    - Exported dump files stored on the hard drive on the AAD Management Workstation
    - A compressed and zipped copy of all of the exported dump files stored on the hard drive on the AAD Management Workstation
    - Exported dump files copied to a rotable pool of ten (10) CD-RW disks.

- Provide for restoring agency data (if necessary) via loading and/or reloading the original CD-R media stored onsite

- Provide for the AAD System Administrator to restore systems software (including Sun Solaris, Oracle, Windows 2000, IIS, PL/SQL Developer, Windows Terminal Server, etc.) via manual means in accordance with the relevant current technical literature such as Sun Solaris, Oracle 10g, and Microsoft technical and reference manuals.

- Provide for the AAD System Administrator to restore and reconfigure operational settings and parameters on switches, firewalls, workstations, drive arrays, and servers via manual means and "best practices" (as necessary).

Table 1. Objects Backed Up on a Daily Basis (Monday – Friday)

Source Subsystem	Objects to be Backed	Logical Formats and Storage Location
Public Subsystem Staff-Only Subsystem Testbed	Metadata and RDT data	1. Exported dump files stored on the hard drive of the onsite Management Workstation 2. Exported dump files saved as a compressed and zipped file on the hard drive of the onsite Management Workstation 3. Exported dump files copied onto a rotable pool of ten (10) CD-RWs which in turn are stored onsite
	User profiles	
	AAD Project documents	
	Scripts and source code including: • Control files for data loading • SQL files for data loading • Load reports • Export scripts • ASP/JSP source code and development folders	
	Triggers, functions, views, sequences, stored procedures, indexes, statistics	
	Event log and query log	
	Oracle Auditing information	
	Agency scanned documentation files	
Management Workstation	Shutdown script(s)	

5.1.7.2 Biweekly Backup and Recovery

The vendor shall perform biweekly backups of the full AAD system to encompass the latest daily backup as defined above. Additional provisions include:

- Review, develop, and deliver a Backup and Recovery Plan as mutually agreed and approved in a time frame mutually agreed upon.

- Backup operational settings and parameters on switches, firewalls, disk arrays, servers, and workstations (including the management workstation and the CM workstation) onto removable CD-RW media mirroring a directory structure consistent with the NARA SDLC and the configuration tool.

- Backup agency data on the NARA staff-only subsystem onto magnetic tape as a database image to enable restoration of agency data on the NARA staff-only system without having to load and/or reload from the original CD-Rs. The exception will be any new agency data loaded via CD-R since the last biweekly backup.

- Provide for the System Administrator to manually restore agency data on the public subsystem (if necessary) via replication of agency data tables from the NARA-staff only subsystem under the control of the backed up AAD Configuration and Object Database (as necessary).

- Continue to provide for the AAD System Administrator to restore systems software (including Sun Solaris, Oracle, Windows 2000, IIS, PL/SQL Developer, Windows Terminal Server, etc.) via manual means in accordance with the relevant current technical literature such as Sun Solaris, Oracle 10g, and Microsoft technical and reference manuals.

- Provide for on-site storage of the bi-weekly backup media with a mutually agreed upon cycle of magnetic tape cartridges and CD-RWs.

5.1.7.3 Disaster Recovery Planning

The vendor shall perform backups of the full AAD system at a mutually agreed upon schedule (TBD) to encompass the daily and biweekly backups as defined above. The vendor shall review the current Disaster Recovery Plan and recommend revisions if necessary. As part of the development or revision of the Disaster Recovery Plan, the vendor shall develop and present an alternative plan for potentially building a “hot” failover site to provide for business continuity.

Additional backup and recovery provisions include:

- Full integration of the configuration tool to overall AAD system operations (including trouble reports, change requests, configuration controls, and baselines) and perform backups of all objects and data managed under the configuration tool.

- Backup agency data on both the NARA staff-only subsystem and the public subsystem onto magnetic tape as database images to enable restoration of all agency data on both subsystems without loading and/or reloading of the original CD-Rs. The exception will be any new agency data loaded via CD-R since the last backup.

- Provide for onsite storage of all backup materials to enable rapid recovery should equipment not be physically compromised or damaged.

- As approved by NARA, store all necessary backup materials (including duplicate copies of all necessary applications, system software, and documentation) off-site and out-of-area to be able to reconstitute the system should there be a disaster that destroys equipment at the vendor's facility.

5.2 Application Development Services

5.2.1 System Enhancements and New Development Projects

As directed by NARA, the vendor will add functionality to the AAD application as future enhancements to support the search and retrieval of electronic records in accordance with NARA's Configuration Management Plan (CMP). The vendor will provide cost estimates and perform application development, system testing, and deployment as required and specified in new delivery orders, the Decision Memorandum (DM) adjudication process, and the change request process defined in the CMP. With each new release of AAD, the vendor will need to revise the Requirements Document and DSDD and submit them to NARA.

As new requirements are defined, the vendor will provide the NARA AAD Project Manager with time estimates for development tasks and will establish reasonable project schedules and delivery dates in accordance with the NARA Configuration Management process. Until the change request process is implemented using the configuration management tool, requests for changes and system enhancements will be accomplished via delivery orders and the DM process. The vendor will maintain and update the schedule for DM implementation on a monthly basis on the AAD Web site.

5.2.2 Patches and Bug Fixes

In coordination with the NARA AAD Project Manager, the vendor will apply software patches and bug fixes to the AAD application as necessary and as required. This effort shall include the following:

- On a monthly basis, the vendor will evaluate any new patches and bug fixes from systems and application software vendors and take action as necessary and as appropriate to install the patch/fix.

The vendor will install critical security patches and fixes or provide justification for not doing so within three business days of notification. **Note:** one justification for not doing so might be the need to conduct an engineering analysis of the need for the patch or to test the patch first within the AAD testbed.

5.2.3 Testbed Services

The vendor will operate and maintain a logically-separate AAD testbed to serve as an environment to develop and demonstrate reusable IT architectural components including systems, applications, interfaces, software, and tools.

5.3 Production Control Services

5.3.1 NARA Onsite Support Services

To complement the vendor AAD Project Manager, the vendor will designate contacts onsite at NARA for NWME to request services, to report problems, to coordinate and manage the docket for metadata completion, to assist in the process for promoting archival series and file units to the public, to provide training, and to provide consultation and outreach on the AAD system to staff and visitors.

The vendor will also provide onsite support at NARA for the following:

- Completing metadata in accordance with the SOM
- Copying agency data files and transferring them via CD-R media to the AAD site
- Scanning and converting Agency- and NARA-produced documentation

5.3.2 System Operations and Maintenance

The vendor will provide onsite and offsite services in accordance with the Systems Operation Manual (SOM).

6. Service Levels

This section of the SLA identifies the services (and the level of service) to be provided by the vendor.

6.1 Data Center Services

SERVICE	SERVICE LEVEL AND PERFORMANCE RANGE		
	Acceptable (Green Zone)	Marginal (Yellow Zone)	Unsatisfactory (Red Zone)

SERVICE	SERVICE LEVEL AND PERFORMANCE RANGE		
	Acceptable (Green Zone)	**Marginal (Yellow Zone)**	**Unsatisfactory (Red Zone)**
Staff-Only Subsystem Availability	98% availability for NARA staff during normal business hours in any given week Normal NARA business hours are defined as Monday through Friday, 8:00 am to 5:00 pm (Eastern Time), excluding Federal holidays In measuring the availability, the AAD staff-only subsystem shall not be down, nor functioning at an unacceptable level of service, for more than 1 hour (total) every 40 hours of normal (business) operation. Time associated with prior scheduled and approved maintenance shall not be included in the downtime availability determination See limitations in Section 5.0 on factors outside of the control of the AAD Project	< 98% availability > 1 hour (total) non-availability during a 40 hour business week	< 95% availability > 2 hours (total) non-availability during a 40 hour business week
Public Subsystem Availability	98% availability for public users accessing the system via the Internet during defined business hours in any given month For the public subsystem, AAD shall be available 365 days/year, - 24 hours/day, 7 days/week (e.g. 365x24x7). In measuring the availability, the AAD public subsystem shall not be down, nor functioning at an unacceptable level of service, for more than 16 hours (total) every month Time associated with prior scheduled and approved maintenance shall not be included in the downtime availability determination See limitations in Section 5.0 on factors outside of the control of the AAD Project	< 98% availability > 16 hours (total) non-availability during a month	< 95% availability > 36 hours (total) non-availability during a month

SERVICE	SERVICE LEVEL AND PERFORMANCE RANGE		
	Acceptable (Green Zone)	**Marginal (Yellow Zone)**	**Unsatisfactory (Red Zone)**
Testbed and CM Server (e.g., PVCS Dimensions) Availability	98% availability during normal business hours in any given week Normal NARA business hours are defined as Monday through Friday, 8:00 am to 5:00 pm (Eastern Time), excluding Federal holidays In measuring the availability, the testbed and CM server shall not be down for more than 1 hour (total) every 40 hours of normal (business) operation. Time associated with prior scheduled and approved maintenance shall not be included in the downtime availability determination See limitations in Section 5.0 on factors outside of the control of the AAD Project	< 98% availability > 1 hour (total) non-availability during a 40 hour business week	< 95% availability > 2 hour (total) non-availability during a 40 hour business week
Provide Configuration Management services and maintain the baseline configuration of the AAD technical environment	Qualitative assessment to be provided by NARA AAD Project Manager at Monthly SLA Review	Qualitative assessment to be provided by NARA AAD Project Manager at Monthly SLA Review	Qualitative assessment to be provided by NARA AAD Project Manager at Monthly SLA Review
Provide the updated docket of metadata completion activity on a weekly basis	NLT 12:00PM on the following Monday	NLT COB on the following Monday	Later than COB on the following Monday
Provide weekly statement affirming continuing system security and data integrity (including software integrity) and any integrity checks performed during the previous week	COB on Monday for the prior week	NLT COB on Tuesday for the prior week	Later than COB on Tuesday for the prior week
Provide weekly statement affirming that required backups have been performed during the week	COB on Monday for the prior week	NLT COB on Tuesday for the prior week	Later than COB on Tuesday for the prior week
Provide weekly report on statistics on public use of the system	COB on Tuesday for the prior week	NLT COB on Wednesday for the prior week	Later than COB on Wednesday for the prior week
Provide monthly rollup report regarding system security and data integrity	NLT five (5) business days after the end of the month	NLT seven (7) business days after the end of the month	NLT ten (10) business days after the end of the month
Provide monthly rollup report regarding system backups	NLT five (5) business days after the end of the month	NLT seven (7) business days after the end of the month	NLT ten (10) business days after the end of the month
Provide monthly rollup report on public statistics	NLT five (5) business days after the end of the month	NLT seven (7) business days after the end of the month	NLT ten (10) business days after the end of the month

SERVICE	**SERVICE LEVEL AND PERFORMANCE RANGE**		
	Acceptable (Green Zone)	**Marginal (Yellow Zone)**	**Unsatisfactory (Red Zone)**
Provide monthly synopsis of trouble reports made during the month	NLT five (5) business days after the end of the month	NLT seven (7) business days after the end of the month	NLT ten (10) business days after the end of the month
Provide monthly report with a synopsis of SLA exceptions taken during the month	NLT five (5) business days after the end of the month	NLT seven (7) business days after the end of the month	NLT ten (10) business days after the end of the month
Generate and deliver *ad hoc* SLA exception reports on an as required basis when service-level targets are not being met and when it first becomes apparent that a service level metric is not being achieved	Provide SLA exception report within 1 business day of exception	Provide SLA exception report within 2 business days of the exception	Provide SLA exception report after 2 business days or fail to provide report
Conduct *ad hoc* queries of server and firewall logs and provide reports as requested by the NARA AAD Project Manager	Provide on time query report as requested by NARA AAD Project Manager and as mutually agreed	Provide 1 day late	Provide 2 days late
Conduct monthly service-level reviews with the NARA AAD Project Manager	Conduct review NLT seven (7) business days after the end of the month	Conduct review more than seven (7) business days but within ten (10) business days after the end of the month	Conduct review more than (10) business days after the end of the month
Monitor and inspect logs on a daily basis IAW 5.1.2.1	Perform daily NLT 12:00 PM	Perform daily NLT 5:00 PM	Miss one or more days
Monitor and manage AAD hardware IAW 5.1.2.2	Qualitative assessment to be provided by NARA AAD Project Manager at Monthly SLA Review	Qualitative assessment to be provided by NARA AAD Project Manager at Monthly SLA Review	Qualitative assessment to be provided by NARA AAD Project Manager at Monthly SLA Review
Monitor and tune performance IAW 5.1.2.3	Qualitative assessment to be provided by NARA AAD Project Manager at Monthly SLA Review	Qualitative assessment to be provided by NARA AAD Project Manager at Monthly SLA Review	Qualitative assessment to be provided by NARA AAD Project Manager at Monthly SLA Review
Manage AAD network services IAW 5.1.3	Qualitative assessment to be provided by NARA AAD Project Manager at Monthly SLA Review	Qualitative assessment to be provided by NARA AAD Project Manager at Monthly SLA Review	Qualitative assessment to be provided by NARA AAD Project Manager at Monthly SLA Review
Manage the database environment IAW 5.1.4	Qualitative assessment to be provided by NARA AAD Project Manager at Monthly SLA Review	Qualitative assessment to be provided by NARA AAD Project Manager at Monthly SLA Review	Qualitative assessment to be provided by NARA AAD Project Manager at Monthly SLA Review
Manage the server environment IAW 5.1.5	Qualitative assessment to be provided by NARA AAD Project Manager at Monthly SLA Review	Qualitative assessment to be provided by NARA AAD Project Manager at Monthly SLA Review	Qualitative assessment to be provided by NARA AAD Project Manager at Monthly SLA Review
Provide physical security IAW 5.1.6.1	Qualitative assessment to be provided by NARA AAD Project Manager at Monthly SLA Review Provide report of material physical security compromise within two (2) hours of discovery	Qualitative assessment to be provided by NARA AAD Project Manager at Monthly SLA Review Provide report of material physical security compromise on the same day as the discovery	Qualitative assessment to be provided by NARA AAD Project Manager at Monthly SLA Review Provide report of material physical security compromise more than a day late or not at all

SERVICE	SERVICE LEVEL AND PERFORMANCE RANGE		
	Acceptable (Green Zone)	**Marginal (Yellow Zone)**	**Unsatisfactory (Red Zone)**
Provide network security IAW 5.1.6.2 for the staff-only subsystem and the public subsystem	Qualitative assessment to be provided by NARA AAD Project Manager at Monthly SLA Review Monitor and review network logs NLT 12:00 PM Provide report of network security compromise within two (2) hours of discovery	Qualitative assessment to be provided by NARA AAD Project Manager at Monthly SLA Review Monitor and review network logs daily NLT 5:00 PM Provide report of network security compromise on the same day as the discovery	Qualitative assessment to be provided by NARA AAD Project Manager at Monthly SLA Review Miss one or more days in monitoring network logs Provide report of network security compromise more than a day late or not at all
On a daily basis, examine Oracle Auditing Tool logs to look for any unauthorized changes to data tables associated with agency electronic records	Qualitative assessment to be provided by NARA AAD Project Manager at Monthly SLA Review Monitor and review Oracle Audit Tool logs NLT 12:00 PM each day Provide report of records integrity compromise within two (2) hours of discovery	Qualitative assessment to be provided by NARA AAD Project Manager at Monthly SLA Review Monitor and review Oracle Audit Tool logs daily NLT 5:00 PM Provide report of records integrity compromise on the same day as the discovery	Qualitative assessment to be provided by NARA AAD Project Manager at Monthly SLA Review Miss one or more days in monitoring network logs Provide report of records integrity compromise more than a day late or not at all
On a weekly basis, examine Oracle Auditing Tool logs for unauthorized changes to functions, stored procedures, triggers, and sequences	Qualitative assessment to be provided by NARA AAD Project Manager at Monthly SLA Review Monitor and review Oracle Audit Tool log NLT 2:00 PM on Monday Provide report of records integrity compromise within two (2) hours of discovery	Qualitative assessment to be provided by NARA AAD Project Manager at Monthly SLA Review Monitor and review Oracle Audit Tool log skipping no more than one day Provide report of records integrity compromise on the same day as the discovery	Qualitative assessment to be provided by NARA AAD Project Manager at Monthly SLA Review Skip two or more days in monitoring and reviewing the Oracle Audit Tool log Provide report of records integrity compromise more than a day late or not at all
On a weekly basis, verify the integrity of AAD applications code in public and staff-only subsystems	Qualitative assessment to be provided by NARA AAD Project Manager at Monthly SLA Review Complete verification NLT 2:00 PM on Monday Provide report of code compromise within two (2) hours of discovery	Qualitative assessment to be provided by NARA AAD Project Manager at Monthly SLA Review Complete verification skipping no more than one day Provide report of code compromise on the same day as the discovery	Qualitative assessment to be provided by NARA AAD Project Manager at Monthly SLA Review Skip two or more days in completing the verification Provide report of code compromise more than a day late or not at all
Perform daily backups IAW 5.1.7.1	Perform backup NLT COB each day	Miss one (1) day	Miss two (2) or more days
Perform biweekly backups IAW 5.1.7.2 and a formal backup and recovery plan	Commence the required backups and other tasking in 5.1.7.2 NLT March 7, 2003 Other metrics TBD	Commence the required backups and other tasking after March 14, 2003 Other metrics TBD	Commence the required backups and other tasking after March 21, 2003 Other metrics TBD
Perform biweekly backups IAW 5.1.7.3 and a formal disaster recovery plan	Commence the required backups and other tasking in 5.1.7.3 NLT April 15, 2003 Other metrics TBD	Commence the required backups and other tasking after April 15, 2003 Other metrics TBD	Commence the required backups and other tasking after April 22, 2003 Other metrics TBD
Level 1 Problem Resolution IAW 7.1.1	Notify NARA PM < 1 hour Fix < 1 hour	Notify NARA PM < 2 hours Fix < 2 hours	Notify NARA PM > 2 hours Fix > 2 hours
Level 2 Problem Resolution IAW 7.1.2	Notify NARA PM < 4 hours Fix < 24 hours	Notify NARA PM < 8 hours Fix < 48 hours	Notify NARA PM > 8 hours Fix > 48 hours

SERVICE	SERVICE LEVEL AND PERFORMANCE RANGE		
	Acceptable (Green Zone)	**Marginal (Yellow Zone)**	**Unsatisfactory (Red Zone)**
Level 3 Problem Resolution IAW 7.1.3	Notify NARA PM < 8 hours Fix < 3 business days	Notify NARA PM < 16 hours Fix < 5 business days	Notify NARA PM > 16 hours Fix > 5 business days
Level 4 Problem Resolution IAW 7.1.4	Notify NARA PM < 16 hours Fix < 5 business days	Notify NARA PM < 24 hours Fix < 10 business days	Notify NARA PM < 32 hours Fix < 10 business days

6.2 Software Development Services

SERVICE	SERVICE LEVEL AND PERFORMANCE RANGE		
	Acceptable (Green Zone)	**Marginal (Yellow Zone)**	**Unsatisfactory (Red Zone)**
Add functionality to the AAD application as enhancements as mutually agreed by the NARA AAD PM and the vendor	Required action(s) completed on time	Required action(s) completed > 1 week late	Required action(s) completed > 2 weeks late
Provide cost estimates and perform application development, system testing, and deployment as required and as specified in new Task 5 delivery orders and the Decision Memorandum (DM) adjudication process.	Required action(s) completed on time	Required action(s) completed > 1 week late	Required action(s) completed > 2 weeks late
Maintain and update the schedule for Decision Memorandum adjudication and implementation on a monthly basis	Action completed by the end of each month	Action completed > 3 business days late	Action completed > 7 business days late
On a monthly basis, evaluate any new patches and bug fixes from system and application software vendors and take action as necessary and appropriate to install the patch/fix (including coordinating with the NARA Project Manager)	Action completed by the end of each month	Action completed > 3 business days late	Action completed > 7 business days late
Install critical security patches and fixes	Critical security patches and fixes installed or justification report for not doing so provided < 72 hours after notification	Critical security patches and fixes installed or justification report for not doing so provided 72 – 120 hours after notification	Critical security patches and fixes installed or justification report for not doing so provided > 120 hours after notification
Operate and maintain a logically separate AAD testbed to serve as an environment to develop and demonstrate reusable IT architectural components.	Qualitative assessment to be provided by NARA AAD Project Manager at Monthly SLA Review	Qualitative assessment to be provided by NARA AAD Project Manager at Monthly SLA Review	Qualitative assessment to be provided by NARA AAD Project Manager at Monthly SLA Review

6.3 Production Control Services

SERVICE	**SERVICE LEVEL AND PERFORMANCE RANGE**		
	Acceptable (Green Zone)	**Marginal (Yellow Zone)**	**Unsatisfactory (Red Zone)**
Perform data loading and reloading (per CD) – assuming no difficulties necessitating development of a new Decision Memorandum (DM). Also, assumes no problems associated with record counts.	Within 2 business days after receipt of media or reload request.	Within 2 - 5 business days after receipt of media or reload request	More than 5 business days after receipt of media or reload request
User Account Maintenance (Per request)	Processed on same business day assuming receipt of the request before 12:00 PM Eastern Processed next business day assuming receipt of the request after 12:00 PM Eastern time	Processed one (1) business day late	Processed two (2) or more business days late
Index columns newly declared to be Quicksearch columns after data load	Within 1 business day	Within 2 – 3 business days	More than 3 business days
Replicate and promote data files to the public subsystem from the public staging server in lots of 8 data files per day.	Within 1 business day after receipt of request to promote the file to public	Within 2 business days after receipt of request to promote the file to public	More than 2 business days after receipt of request to promote the file to public
Delete (e.g., purge) files and tables from the AAD system at the direction of the NARA AAD Project Manager	< 2 hours during normal business hours after receipt of notification for deletions declared to be urgent < 8 business hours for all other requests	2 – 4 hours during normal business hours after receipt of notification for deletions declared to be urgent 8 – 16 business hours for all other requests	> 4 hours during normal business hours after receipt of notification for deletions declared to be urgent > 16 business hours for all other requests

7. Problem Resolution and Response Times

Each problem that results in a trouble report (see Section 4.1 of this SLA) shall be assigned a priority for problem resolution in accordance with this section of the SLA.

7.1 Priority Levels for Trouble Resolution

7.1.1 Level 1 Problems

The system is *disabled*, causing mission-critical impact to AAD operations if the service is not restored quickly. The vendor will assign sufficient resources to resolve the problems as quickly as possible with the goal of restoring and maintaining the service levels agreed to in this document. By "*disabled*", it is meant that **none** of the modules (e.g., MCT, RDT, BSR) work. Also, if the public Browse, Search, and Retrieval (BSR) module is not working **at all**, this situation constitutes a Level 1 problem.

The nominal target for resolution of Level 1 problems is 1 hour or less; however this target cannot be guaranteed especially for complex problem involving the network, prolonged loss of power, the potential for Internet or security disruptions (including denial of service attacks), or problems outside of the control of the AAD Project as discussed in Section 5.0. However, for Level 1 problems the vendor will work in good faith and use continuous effort to resolve the problem until an acceptable fix is installed and tested and until the system is back to normal operations.

Level 1 problems will be continuously monitored and NARA will be notified of the status via periodic updates to the trouble report form and via manual means (e.g., e-mail or voice). For Level 1 problems, during normal business hours of operations, the target for notification of the NARA Project Manager will be 1 hour starting at the time that the problem is first reported by either NARA or vendor personnel.

7.1.2 Level 2 Problems

The public BSR module is *severely degraded*. An example of a Level 2 problem is if the public is experiencing Internet errors (File 404 or 500) or other issues where the public is unable to use the public BSR effectively. Level 2 problems that have no workarounds will have a target resolution of 24 hours depending on the corrective actions required to return the system to normal operations. The vendor will communicate these corrective actions and resolution timeframes to NARA. The vendor will assign sufficient resources to fix the problem in the target resolution timeframe.

For Level 2 problems, during normal business hours of operations, the target for notification of the NARA project manager will be 4 hours starting at the time that the problem is first reported to either NARA or vendor personnel.

For Level 2 problems, the vendor will work to resolve the problem and will attempt to provide a solution within 24 hours after problem identification. Any deviations from this service level of commitment will normally be authorized in advance by the NARA PM. Subsequently they must be explained and justified in an SLA exception report.

7.1.3 Level 3 Problems

The system is severely degraded, impacting one of the following modules: 1) loss of metadata entry/edit capability, or 2) loss of RDT capability, or 3) loss of Browse, Search and Retrieval (BSR) capability for the NARA-staff only subsystem (including the public staging server).

The public BSR system is degraded. Network and/or system performance is noticeably impaired, but most AAD operations can continue. Level 3 problems will have a target resolution of 3 business days unless otherwise specified by the vendor (and agreed to by NARA) for a particular problem.

For Level 3 problems, during normal business hours of operations, the target for notification of the NARA AAD Project Manager will be within 1 business day (e.g., 8 business hours) starting at the time that the problem is first reported by either NARA or vendor personnel.

For Level 3 problems, the vendor will work to resolve the problem and will attempt to provide an acceptable solution or a workaround within three (3) business days after problem identification. Any deviations from this service level of commitment will normally be authorized in advance by the NARA PM. Subsequently they must be explained and justified in an SLA exception report.

7.1.4 Level 4 Problems – Bug Fixes and Nuisance Errors

The system is operational and performing normally with perhaps the exception of a particular series or data file non-operational due to a metadata error. Alternately, NARA discovers a bug or a nuisance error in the system.

For Level 4 problems, during normal business hours of operations, the target for notification of the NARA AAD Project Manager will be within 2 business days (e.g., 16 business hours) starting at the time that the problem is first reported by either NARA or vendor personnel.

The vendor will research such errors on request from NARA with the goal of fixing the error within 5 business days. If the error or bug can not be reasonably resolved within 5 business days, the vendor will provide a response back to the originator with a copy to the NARA AAD Project Manager indicating that the problem is more severe with an estimate of the timeframe to resolve the error.

Appendix A: Trouble Report Template

Name: ____

Subject: ____

Report Number (to be assigned by vendor): _______________

Priority for Resolution (to be determined by the onsite vendor team lead)
(Please check per section 7.1 in the SLA)

___ Level 1 (Mission Critical)

___ Level 2 (Major subsystem or module loss)

___ Level 3 (Degraded performance)

___ Level 4 (Bug fix or nuisance error)

Type of Report (Please check):

___ Initial report of trouble (Sequence number is 1, e.g., this is the 1st report in this sequence)

___ Follow-on information to previous report of trouble (Increase previous sequence number by one (1) e.g., this is the 2nd report in this sequence)

___ Closure (For vendor use)

Sequence Number: _________

Date problem first noted: ________________

Time problem first noted: ________________

Where was the problem noted in the system? (e.g., which page and on which subsystem or module) Example: Search results page on the NARA staff-only browse, search, and retrieval module):

____

____

____

____

Is the problem repeatable? (Please check)

___ YES

___ NO

___ UNCERTAIN or DO NOT KNOW

Does the problem appear to be limited to a particular series or file unit?
(Please check)

___ YES (If so, which series and file unit?

Series: ____

File Unit: ____

___ NO

___ UNCERTAIN or DO NOT KNOW

Nature of the Problem: Please describe:

____

____

____

____

____

What is your browser type and version number? (Please check)

___ Internet Explorer (Version __________)

___ Netscape (Version _____________)

Are there any special circumstances that you noticed? If so, please describe.

____

____

____

Notes:

Screenshots: Please attach screenshots of the AAD window if appropriate
(via: *ALT-Print screen* and *Edit-Paste* operation)

Attach screenshots here

Vendor Response to Trouble Report

Report Number: ______________

Service Level Metric Impacted and Extent of Impact:

Prognosis and Expected Results:

Expected Date/Time of Resolution:

Projected Date for Resolution: __________________________

Projected Time for Resolution: __________________________

Expected Results:

Personnel Assigned:

Closeout Information:

Appendix B: SLA Exception Report Template

Subject of Exception Report: ____

Date Exception First Noted: ________________

Time Exception First Noted: ________________

Service Impacted by the Exception:

____

____

____

____

Level of Exception: (Please check)

___ YELLOW

___ RED

Nature of the SLA Exception:

____

____

____

____

Circumstances of the Exception (Including Mitigating Circumstances):

____

____

____

____

Personnel Assigned and Actions Implemented by vendor:

____

____

____

____

Requested Actions of vendor (if any):

Prognosis for Resolution of the SLA Exception:

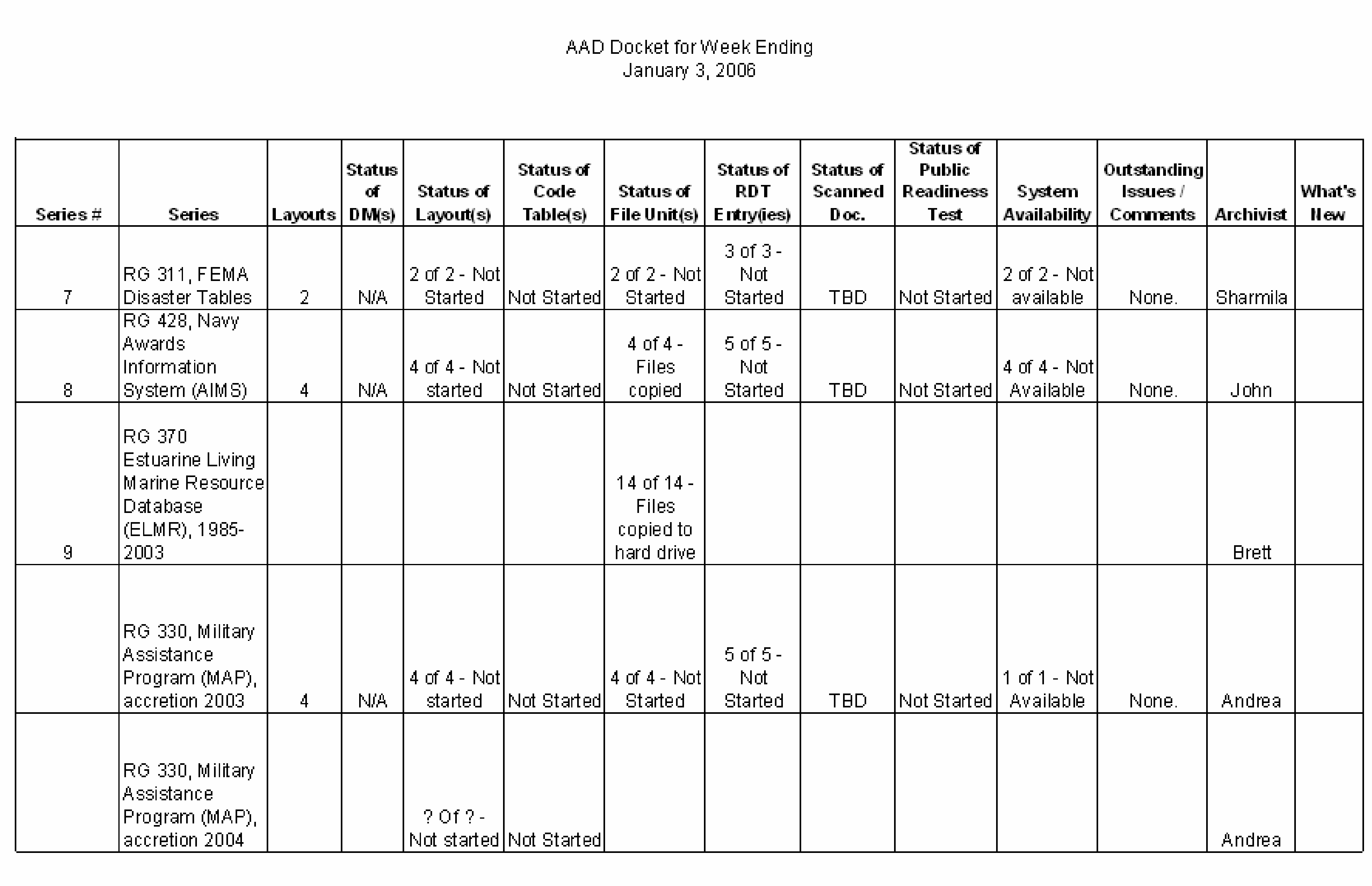
Expected Date/Time for Return to Green Status:

Projected Date for Return to Green: __________________________

Projected Time for Return to Green: __________________________

Prognosis:

Appendix C: AAD Docket Template with Sample Data



AAD Docket for Week Ending
January 3, 2006

Series #	Series	Layouts	Status of DM(s)	Status of Layout(s)	Status of Code Table(s)	Status of File Unit(s)	Status of RDT Entry(ies)	Status of Scanned Doc.	Status of Public Readiness Test	System Availability	Outstanding Issues / Comments	Archivist	What's New
7	RG 311, FEMA Disaster Tables	2	N/A	2 of 2 - Not Started	Not Started	2 of 2 - Not Started	3 of 3 - Not Started	TBD	Not Started	2 of 2 - Not available	None.	Sharmila	
8	RG 428, Navy Awards Information System (AIMS)	4	N/A	4 of 4 - Not started	Not Started	4 of 4 - Files copied	5 of 5 - Not Started	TBD	Not Started	4 of 4 - Not Available	None.	John	
9	RG 370 Estuarine Living Marine Resource Database (ELMR), 1985-2003					14 of 14 - Files copied to hard drive						Brett	
	RG 330, Military Assistance Program (MAP), accretion 2003	4	N/A	4 of 4 - Not started	Not Started	4 of 4 - Not Started	5 of 5 - Not Started	TBD	Not Started	1 of 1 - Not Available	None.	Andrea	
	RG 330, Military Assistance Program (MAP), accretion 2004			? Of ? - Not started	Not Started							Andrea	

Appendix D: Statistics on Public Use Report Template

Number of "Virtual Visitors" (Number of Sessions) for Week Ending ____________

Number of Sessions	Day of Week						
	Sunday MM/DD	Monday MM/DD	Tuesday MM/DD	Wednesday MM/DD	Thursday MM/DD	Friday MM/DD	Saturday MM/DD
	X	X	X	X	X	X	X

Number of Queries Executed on a Series-by-Series Basis for Each Day during the Week Ending _______________

Series Name	Day of Week						
	Sunday MM/DD	Monday MM/DD	Tuesday MM/DD	Wednesday MM/DD	Thursday MM/DD	Friday MM/DD	Saturday MM/DD
RG XXX, Title	X	X	X	X	X	X	X
RG XXX, Title	X	X	X	X	X	X	X
RG XXX, Title	X	X	X	X	X	X	X

Number of successful queries per series per week by top level domain name [.com, .edu, .gov (excluding .nara.gov), .mil, .nara.gov, .net, .org, OTHER (none of the previous, but known), UNKNOWN] for logged user IPs for the Week Ending ________.

Series Title	.com	.edu	.gov	.local.saic	.mil	.nara.gov	.net	.org	OTHER	UNKNOWN	Week Totals
RG XXX, Title	X	X	X	X	X	X	X	X	X	X	X
RG XXX, Title	X	X	X	X	X	X	X	X	X	X	X
RG XXX, Title	X	X	X	X	X	X	X	X	X	X	X

Web Server and Database Server Performance Statistics for Each Day during the Week Ending _______________

Day of Week: Sunday (et al) MM/DD/YY

	2/13/2006	2/14/2006	2/15/2006	2/16/2006	2/17/2006	2/18/2006	2/19/2006
AVG of simultaneous users	X	X	X	X	X	X	X
AVG Records Returned	X	X	X	X	X	X	X
AVG Query Time	X	X	X	X	X	X	X
AVG Time to First Byte	X	X	X	X	X	X	X
AVG Time to Last Byte	X	X	X	X	X	X	X
MAX simultaneous users	X	X	X	X	X	X	X
MAX Records Returned	X	X	X	X	X	X	X
MAX Query Time	X	X	X	X	X	X	X
MAX Time to First Byte	X	X	X	X	X	X	X
MAX Time to Last Byte	X	X	X	X	X	X	X

Number of Invalid Queries for Each Day during the Week Ending ______________

Day of Week	Number Unsuccessful
Sunday, MM/DD	X
Monday, MM/DD	X
Tuesday, MM/DD	X
Wednesday, MM/DD	X
Thursday. MM/DD	X
Friday, MM/DD	X
Saturday, MM/DD	X
Weekly Total	Total

Number of Times Scanned Technical Information Package Items are Downloaded for Each Day during the Week Ending ________

Day of Week	Number of Technical Information Package Downloads
Sunday, MM/DD	X
Monday, MM/DD	X
Tuesday, MM/DD	X
Wednesday, MM/DD	X
Thursday. MM/DD	X
Friday, MM/DD	X
Saturday, MM/DD	X

Weekly Total	**Total**

Number of Times Search Results are Downloaded as .csv Files for Each Day during the Week Ending ________

Day of Week	Number of .CSV File Downloads
Sunday, MM/DD	**X**
Monday, MM/DD	**X**
Tuesday, MM/DD	**X**
Wednesday, MM/DD	**X**
Thursday. MM/DD	**X**
Friday, MM/DD	**X**
Saturday, MM/DD	**X**
Weekly Total	**Total**

Appendix E: Other Report Templates

System Security and Data Integrity

Narrative statement affirming continuing system security and data integrity (including software integrity) and any integrity checks performed. The weekly report will be for a week interval (Sunday through Saturday). The monthly report will be for a calendar month.

System Backups

Narrative statement affirming that required backups have been made. The weekly report will be for a week interval (Sunday through Saturday). The monthly report will be for a calendar month.

Synopsis of Trouble Reports Made During the Month

Number During Month:	Priority Level			
	Level 1	Level 2	Level 3	Level 4
New	X	X	X	X
Closed Out	X	X	X	X
Remaining Open	X	X	X	X
Average Response Time	X	X	X	X

Synopsis of SLA Exception Reports Made During the Month

Number During Month:	Level of Exception Status	
	Yellow	Red
New		
Returned to Green		
Remaining Exceptions		
Average Time to Return to Green Status		

Monthly Audit Log Summaries

Narrative statement that audit logs were monitored as required for unauthorized changes to: data tables associated with agency electronic records, functions, stored procedures, triggers, and sequences. Any incident(s) will be detailed and the actions that were taken will be documented.

Firewall and Intrusion Detection System (IDS) Reports

Narrative statement that there were no firewall or other intrusions. Any incident(s) will be detailed and the actions that were taken will be documented.

Alerts and Patches Implemented

Narrative statement indicating alerts and patches that were implemented during the month.

Configuration Status Accounting Report (CSAR)

1	2	3	4	5	6	7	8	9	10	11
Contract Reference Number[1]	Product Name[2]	CII[3]	Milestone[4]	Baseline[5]	Planned Delivery Date[6]	Developer’s Approval Authority[7]	AAD Reviewers[8]	Reviews Complete[9]	AAD Approval Authority[10]	Status[11]

The AAD contract CM representative shall populate this CSAR on monthly basis. The Project CM Rep shall maintain this report throughout the life of the project. The AAD project manager will supply the name of the AAD Approval Authority for each deliverable if they differ. Products that are delivered at multiple points in time shall be entered once per delivery occurrence. As this CSAR is completed/updated, it will be distributed to the appropriate recipient

[1] If the deliverable is referenced in the contract or task order, provide the reference

[2] Provide the exact name of the product

[3] Provide the Configuration Identification Item number(CI) based on standard naming convention outlined in the CMP

[4] If the product is part of a milestone deliverable, then provide the milestone designator; i.e., 2, 3, 4

[5] If the product is part of a baseline, then provide the baseline designator; i.e., Functional, Allocated, or Product

[6] Provide the planned delivery date.

[7] Provide the name of the individual who is the developers approval authority for the product

[8] Provide the name of each AAD person who will perform a product review

[9] Provide the date that the AAD reviews are scheduled to be completed

[10] The AAD PM will provide the name of the individual who is authorized to approve the product. For Baselined products the named individual will be the chair of the designated PCCB

[11] Enter the actual date of delivery to the AAD for approval/acceptance or such optional information as late, cancelled, delayed until … dependent on …etc